APPROVED FOR RELEASE DATE: 14-Jan-2015

(U~~//FOUO~~) Final Report of the Rendition, Detention, and Interrogation Network Agency Accountability Board

I. (U) Scope of Review

(U~~//FOUO~~) The CIA Office of the Inspector General (OIG) on 30 January 2014 opened an investigation into potential unauthorized access to the Senate Select Committee on Intelligence (SSCI) shared drive portion of the Rendition, Detention, and Interrogation Network (RDINet) based on information derived from a special review conducted on 29 January 2014. The OIG on 3 February 2014 reported to the Department of Justice (DOJ) the matter of potential CIA officer violations of 18 U.S.C. §§ 1030 (Computer Fraud and Abuse Act) and 2511 (Wiretap Act). The DOJ on 8 July 2014 informed the OIG that the DOJ had no prosecutorial interest in the case and the OIG delivered its completed report to the Director of the Central Intelligence Agency (D/CIA) on 18 July 2014.

~~(C//NF)~~ The OIG Report concluded that Office of General Counsel (OGC) officers [redacted] and [redacted], Agency Information Technology (IT) [redacted] officers [redacted] and [redacted], and [redacted] improperly accessed the SSCI Majority Staff shared drive on RDINet. The OIG found the three IT officers also demonstrated a lack of candor during their first interviews with the OIG because they did not disclose actions they took on behalf of the two OGC officers.

(U~~//FOUO~~) The OIG investigated a crimes report filed by the Agency with the DOJ that reported that SSCI staff members may have improperly accessed Agency information on the RDINet. The OIG found that the factual basis for this referral was unfounded and the author of the letter had been provided inaccurate information on which the letter was based.

(U~~//FOUO~~) The OIG also found that subsequent to a directive by the D/CIA to halt the Agency review of SSCI staff access to the

[redacted]

APPROVED FOR RELEASE DATE: 14-Jan-2015

RDINet, [redacted] Security conducted a limited investigation of SSCI activities on the RDINet that included a keyword search of all, and review of some, e-mails of SSCI Majority staff members on that network.

(U/~~/FOUO~~) The D/CIA on 6 August 2014 convened an Agency Accountability Board (the Board) in response to the OIG findings. The Board was commissioned to investigate the conduct of the five individuals referenced in the IG report and provide recommendations regarding both their individual accountability and any systemic CIA issues the Board might find. (A summary of the Board membership is found in Tab A.)

(U/~~/AIUO~~) The Board held its first meeting on 21 August 2014 and completed its deliberations on 24 November 2014. The Board first sought to establish relevant facts concerning the incidents cited in the OIG report per Accountability Board guidance found in Agency Regulation 4-7. As a result, Board members reviewed the OIG report, OIG's Memoranda of Investigative Activity that summarize OIG interviews, written responses to the OIG report from the five named individuals, and other documents provided by individuals or used by the OIG to make its determinations. The Board also interviewed the five named individuals, the D/CIA, the Executive Director, [redacted] the Office of Security (OS), [redacted] the Counterintelligence Center (CIC), [redacted] OIG's investigative staff, the OIG attorney, and OIG officers who conducted the investigation.

(U//~~FOUO~~) This report represents the Board's summary, analysis, and recommendations based on relevant information that came before the Board and is not intended to be a definitive history of the RDI Network. The Board was directed to limit its investigation only to the conduct of Agency officers, not investigate the conduct of SSCI staff members.

A. (U) The RDI Network

(U//~~FOUO~~) The creation of the RDINet was ground-breaking in that it provided SSCI staff members with full, un-redacted access to millions of the Agency's most sensitive operational materials.

APPROVED FOR RELEASE DATE: 14-Jan-2015

The Agency had to build an information system that enabled the review and release of these documents, provide a secure means to transfer the documents to SSCI staff members, and create electronic partitions to offer some protection of SSCI work product.

(U~~//FOUO~~) Most officers interviewed by the Board noted the unprecedented nature of RDINet with two branches of Government using a shared computer network system to distribute vast amounts of sensitive operational information. Regrettably, none of the documents reviewed by the Board contained guidance on procedures to be used in the event of a suspected security incident.

(U~~//FOUO~~) CIA Had Operational Responsibility for RDINet

(U~~//FOUO~~) The Board received a copy of the 8 February 2011 document *DRG-RDI/SSCIRG Handbook for File Reviews* that contains a summary of the RDINet program history. According to the *Handbook*, the SSCI on 26 March 2009 advised then-CIA Director Panetta that the Committee would conduct a thorough review of how the CIA created, operated, and maintained its detention and interrogation program. Director Panetta on 1 May 2009 issued a preservation order directing CIA personnel to save documents, information, records, and other materials related to CIA's detention and interrogation program. The authorized date range for any data under review to be possibly responsive was set as 11 September 2001 to 22 January 2009.

(U~~//FOUO~~) CIA established RDINet at its [redacted] Building facility in June 2009 to allow the Agency to review and release responsive RDI material to SSCI Staff members. At no time was any equipment associated with RDINet located on Senate property, nor was the equipment itself property of the Senate. The Agency used electronic protocols to provide SSCI staff members with access to specific documents located in a database and separate electronic shared drives were established for SSCI Majority and Minority staffs. SSCI staff could only access RDINet by being physically present in the [redacted] building. No remote access from SSCI offices was possible.

APPROVED FOR RELEASE DATE: 14-Jan-2015

(U~~//FOUO~~) CIA Operated and Maintained RDINet

(U~~//FOUO~~) RDINet was operated by the CIA, maintained by CIA staff and contractor IT officers, and CIA staff officers oversaw the implementation of the system when they led what was designated as the Director's Review Group, the Office of Detainee Affairs, or the RDI Review Team.

(U~~//FOUO~~) In addition to the *Handbook*, the Board received Version 2.8 of the RDINet System Security Plan dated 29 August 2013 and a copy of a 15 June 2011 Statement of Work that covers activities of contractors who perform development work on Counter Terrorism Center document management systems that include RDINet.

(U~~//FOUO~~) Combined with the unsigned Memorandum of Understanding (MOU) (discussed under the *No Written Agreement Governed CIA Access to the SSCI Side of RDINet* section below), these four documents capture how the Agency managed the operation of RDINet. According to an overview in the Statement of Work, the Agency designated the highly customized system as Spartan Gate[1] and retained standard security practices, created inter-office document management workflow, permitted redaction referral and review processes, and used standard information dissemination practices.

(U~~//FOUO~~) CIA was Responsible for the Security of RDINet

(U~~//FOUO~~) RDINet contained millions of documents, where were provided without redaction. Therefore, RDINet contains highly classified and compartmented information about intelligence sources and methods; pseudonyms and true names of Agency personnel, assets, liaison officers, and detainees; details about liaison relationships; and, the locations of black sites. The Agency was responsible for securing this highly sensitive material from unauthorized disclosure. Section 102A(i) of the National Security Act requires the Director of National Intelligence (DNI) to protect intelligence sources and methods from unauthorized disclosure. 50 U.S.C. § 3024(i)(1). To accomplish this imperative, the DNI requires "heads of the IC

[1] (U) The Agency creates names for systems to be used as a common reference or as an unclassified name for a classified system.

APPROVED FOR RELEASE DATE: 14-Jan-2015

elements [to] protect national intelligence, intelligence sources, methods and activities from unauthorized disclosure." Intelligence Community Directive 700(E)(2)(a). Executive Order 12333 contains the same imperative to "protect intelligence, intelligence sources, methods, and activities from unauthorized disclosure." EO 12333 § 1.6(d).

(U~~//FOUO~~) Section 1.5 of the RDINet System Security Plan highlights that the protection level and levels-of-concern for RDINet follow guidance in the 5 June 1999 Director of Central Intelligence Directive (DCID) 6/3 Protecting Sensitive Compartmented Information within Information Systems. The policy section of DCID 6/3 contains the following:

> Intelligence information shall be appropriately safeguarded at all times, including when used in information systems. The information systems shall be protected. Safeguards shall be applied such that (1) individuals are held accountable for their actions; (2) information is accessed only by authorized individuals* and processes; (3) information is used only for its authorized purpose(s); (4) information retains its content integrity; (5) information is available to satisfy mission requirements; and (6) information is appropriately marked and labeled.
>
> * Authorized individuals are those with the appropriate clearance, formal access approvals, and need-to-know.

(U~~//FOUO~~) DCID 6/3 goes on to define a security incident as "an act or circumstance in which there is a deviation from the requirements of the governing security regulations. Compromise, inadvertent disclosure, need-to-know violation, and administrative deviation are examples of security incidents."

(U~~//FOUO~~) Section 7.1 on System Administration in the RDINet System Security Plan requires the system administrator to explain how user notifications will be accomplished on the network. The following text listed in the Plan explains how this requirement is satisfied:

> (U~~//FOUO~~) All users of the RDINet will be informed by the application that they consent to monitoring and recording,

APPROVED FOR RELEASE DATE: 14-Jan-2015

and that unauthorized use is prohibited and subject to criminal and civil penalties. The login splash screen for all users fulfills this requirement.

(U~~//FOUO~~) The OIG, [redacted] the CIC, and various interviewees noted that all SSCI users on RDINet clicked the OK button for the login warning banner that read:

> This is a U.S. Government system and shall be used for authorized purposes only. All information on this system is the property of the U.S. Government and may not be accessed without prior authorization. Your use of this system may be monitored and you have no expectation of privacy. (emphasis added) Violation of system security regulations and guidance may result in discipline by the Agency, and violators may be criminally prosecuted.

(U~~//FOUO~~) RDINet was Subject to Comprehensive, Continuous Monitoring for Security Purposes

~~(S//NF)~~ The entirety of RDINet, including the SSCI side, was subject to the same [redacted] monitoring by the CIC's [redacted] as any other Agency information system.[2] The monitoring is routinely conducted as a security and counterintelligence measure.[3]

B. (U) Arrangements for Use of the System

(U) Protection of SSCI Work Product

(U~~//FOUO~~) Documents reviewed by the Accountability Board highlight that SSCI work product was to be protected within RDINet. The Board did not receive, nor understand there to have been, a signed agreement between the SSCI and Agency on the definition of work product. The OIG report included an undated document on the Standard Operating Procedures for SSCI Review

---

[2] (U~~//FOUO~~) OIG Report, ¶ 17.

[3] (U) Ibid.

APPROVED FOR RELEASE DATE: 14-Jan-2015

that contains what the Board considers to have been one understanding of SSCI work product:

> (U~~//FOUO)~~ Any documents generated on the network drive (a walled-off network share-drive), as well as any other notes, documents, draft and final recommendations, reports, or other materials generated by the Committee staff or Members, are the property of the Committee and will be kept at the Reading Room solely for the safekeeping and ease of reference. These documents remain congressional records in their entirety and disposition and control over these records, even after completion of the Committee's review, lies exclusively with the Committee.

(U~~//FOUO)~~ No Written Agreement Governed CIA Access to the SSCI Side of RDINet

(U~~//FOUO)~~ The OIG used correspondence between the SSCI and the Agency to establish what the OIG termed a "common understanding" on the implementation of RDINet. The Board agrees that one can discern a general working agreement on the day-to-day operations of RDINet, but there was no final, clear agreement on access limits to the SSCI portion of the network. On the evidence reviewed by the Board it appears that recognizing the difficulties of reaching a full final agreement, the Senate and the Agency proceeded instead to leave the resolution of issues that arose to ad hoc administrative processes.

(U~~//FOUO)~~ The 2 June 2009 letter from the SSCI Chair and Vice Chair requests the Agency to "provide a stand-alone computer system in the Reading Room with a network drive for Committee staff and members. This network drive will be segregated from CIA networks to allow access only to Committee staff and Members. The only CIA employees or contractors with access to this computer system will be CIA information technology personnel who will not be permitted to copy or otherwise share information from the system with other personnel, except as otherwise authorized by the Committee."

(U~~//FOUO)~~ Director Panetta responded to the SSCI letter on 4 June 2009 with a clarification that "the stand-alone network must be accessed by the CIA staff assigned to this effort to

APPROVED FOR RELEASE DATE: 14-Jan-2015

perform a variety of tasks, including, for example, loading and organizing the raw responsive data requested by the Committee and review or redaction of material sought to be removed from the Reading Room." The Director's letter further outlines that "any remaining security or logistical concerns or other issues can be resolved through our respective staffs."

(U~~//FOUO~~) A letter from Director Panetta to the SSCI Chair on 12 June 2009 notes "an agreement was reached between CIA and SSCI staff personnel regarding operating procedures for the SSCI review of material related to the CIA's detention and interrogation programs." The Board could find no further information that would clarify the substance behind this statement and the OIG could not locate a final signed agreement.

(U~~//FOUO~~) The OIG report included a 28 May 2009 unsigned MOU on SSCI's review of CIA's Detention and Interrogation Program. The SSCI had informed the Agency that it would issue a subpoena to gain access to unredacted documents containing true names, cryptonyms, pseudonyms, liaison provided intelligence, information from other US government organizations, and the identity of "black sites." The Agency decided to avoid protracted litigation and agreed to provide the above-referenced information with a series of conditions that included:

- Responsive information will be available at a secure Agency Reading Room facility which will permit SSCI personnel with electronic search, filing, and print capability.
- All notes, documents, draft and final recommendations, reports, and other materials generated by SSCI must be prepared and stored in the Reading Room on the CIA approved stand-alone computer system provided. A specially designed share-drive will be provided on the Agency's stand-alone network. As SSCI requires, the share-drive can be segregated with only SSCI access and walled-off CIA IT administrators, except as otherwise authorized by SSCI.
- All SSCI personnel will be required to receive and acknowledge receipt of a CIA security briefing prior to beginning the review and will be required to review and sign a standard Sensitive Compartmented Information (SCI)

APPROVED FOR RELEASE DATE: 14-Jan-2015

non-disclosure agreement relating to classified information obligations.

(U~~//FOUO~~) The Parties Dealt with CIA Access to CIA Documents Transferred to the SSCI Side of RDINet on an Ad Hoc Basis. Sometimes They Agreed. Sometimes They Did Not.

(U~~//FOUO~~) In the absence of a written understanding, ad hoc procedures were created as questions on issues arose. Indeed, the January 2014 RDINet incident was not the first time the Agency searched the SSCI side of RDINet to determine if certain CIA-created documents not yet approved for transfer were inappropriately present on the SSCI side of the network. Such administrative searches were commonplace.[4,5,6] For example, on 10 and 11 January 2011, a SSCI staffer asked a CIA officer to search the SSCI side of the database for documents the staffer thought were missing.[7] Another CIA officer responded by e-mail on 21 January 2011 that the cables the SSCI staffer requested were now accessible to SSCI Staff.[8] While a search could reveal that the requested documents had not been produced for transfer to

---

[4](U~~//FOUO~~) CIA [redacted] AAB Submission, p.3 ("There was nothing unusual about a request to determine the presence of files for which the SSCI staff lacked authorized access on the drives used by the SSCI Majority and Minority Staffs. The efforts I undertook at the direction of [redacted] were entirely consistent with my responsibilities for RDINet security.")

[5](U~~//FOUO~~) [redacted] AAB Submission, p. 2 ("On numerous occasions over four-plus years, CIA IT officers had accessed RDI Net as they did here, for the purpose of determining whether particular documents were resident on the system. They often did so at the urging of the Committee staffers themselves, using administrative procedures that were the same or similar to those used in this case. . .")

[6](U~~//FOUO~~) [redacted] AAB submission, p. 5 ("Throughout the SSCI review, SSCI staff knew the practical necessity of carrying out the document production required the non-IT professional CIA staff routinely access CIA-generated documents on the CIA system for the purpose of administering the document production.")

[7](U~~//FOUO~~) [redacted] AAB submission, tab 6. (E-mail dated 10 January 2011 (06:08 PM) from e-mail dated 11 January 2011 (06:12).

[8](U~~//FOUO~~) Ibid. (E-mail dated 21 January 2011 (12:13 PM).

APPROVED FOR RELEASE DATE: 14-Jan-2015

the SSCI staff, it also could reveal that the documents were in fact already on the SSCI side of RDINet.[9]

(U~~//FOUO)~~ Another example is the May 2010 transactions in which the Agency unilaterally removed 926 documents from the SSCI side of RDINet.[10] CIA removed the documents because they had been erroneously comingled before being screened for privilege concerns.[11]

(U~~//FOUO)~~ A SSCI staffer objected to the removal of the documents, making three assertions about documents on RDINet:

1. Documents made available to SSCI on RDINet have been turned over to the Committee, even if made available erroneously;

2. CIA should not unilaterally access documents on the SSCI side of RDINet; and

3. CIA should not unilaterally remove or alter documents on the SSCI side of RDINet.[12]

(U~~//FOUO)~~ The Agency declined to summarily return these documents to the SSCI side of RDINet, and instead, the White House reviewed them for Executive Privilege.[13] When that review was complete, the Agency returned the majority of the documents

---

[9](U~~//FOUO)~~ Ibid. (E-mail dated 23 March 2011 from CIA officer to SSCI staffer ("I checked the SSCI side of Spartan Gate and it appears that [the document you requested] is already in the system.")).

[10](U~~//FOUO)~~ OIG Report Exhibit D, ¶ 2.

[11](U) Ibid.

[12](U) 12 May 2011 (01:31 PM) e-mail from the SSCI staffer to CIA attorneys.

[13](U~~//FOUO)~~ 13 May 2010 (05:36 PM) e-mail from a CIA attorney to [redacted] and a CIA attorney, and the CIA General Counsel ("The WH is not inclined at this point to ask CIA to categorically replace all the documents that were pulled, in large part because the mistake was clerical in nature ... CIA will continue its ongoing efforts to identify all documents that were pulled from the reading room and to produce all such documents to the WHC for review asap.").

APPROVED FOR RELEASE DATE: 14-Jan-2015

to the SSCI side of RDINet, but withheld those subject to the Privilege.[14] This incident reflects an Agency and White House view, known to the SSCI, that the SSCI side of RDINet was non-inviolable. The CIA officials believed that it was permissible for the Agency to search the SSCI side of the database to determine whether particular Agency documents were present there.[15] [redacted] emphasized at the time that such searches would be "limited to checking to see whether a document is or is not already in the reading room."[16] However, at that time, Senator Feinstein expressed to the White House her strong view that removal of documents was inappropriate, and the White House acknowledged her concerns and agreed that the documents should not have been removed without notice to the Senate and no such removals should occur in the future.

(U~~//FOUO~~) General Conclusion: SSCI staffers were, or should have been aware of, CIA's [redacted] monitoring of RDINet for security purposes. In fact, CIA had previously accessed [redacted] collected from the SSCI side of RDINet when security concerns arose.

(a) (U~~//FOUO~~) The Board determined that while an informal understanding existed that SSCI work product should be protected, no common understanding existed about the roles and responsibilities in the case of a suspected security incident.

(b) (U~~//FOUO~~) The joint desire to begin the review and avoid protracted negotiations on a final agreement led the parties to

---

[14] (U~~//FOUO~~) Memo, "Administrative Document Production Error," 1 June 2010.

[15] (U~~//FOUO~~) 7 June 2010 (10:53 AM) e-mail from a CIA attorney to [redacted] ("Occasionally in the course of the White House's review of EP documents, they will come across a document they believe may already be in the reading room (as part of a different batch) and have asked us to check, so they don't assert EP over a document that has already been produced. Prior to last month's events, the SOP was to check the reading room's holdings (electronically - not physically) and let the WH know. We would like to continue to honor WH requests to check the reading room's holding when they ask about a specific document. Are you ok with our continuing to do so? We currently have several requests outstanding.").

[16] (U~~//FOUO~~) 8 June 2010 (01:51 PM) e-mail from a CIA attorney to the RDI Front Office, another CIA officer, and [redacted]

APPROVED FOR RELEASE DATE: 14-Jan-2015

proceed without a definitive, fully executed agreement, they elected instead to handle issues as they arose.

(c) ~~(TS/~~ ~~NF)~~ The Board concluded SSCI staffers were, or should have been, aware of the monitoring by because of past discoveries of SSCI staffers' misconduct on RDINet:

~~(TS/~~ ~~/NF)~~ In December 2009, the monitoring detected that a SSCI staffer In January 2010, the same individual also reported having a camera in the secure facility to the facility's gate guard but did not provide the camera for review. The individual was identified as on RDINet in November and December 2010. The matter was referred to the CIA Counterintelligence Center's Counterespionage Group (CEG) and the employee was removed from the SSCI team.[17]

~~(TS/~~ ~~/NF)~~ In May 2010, a SSCI staff member requested from the Agency the ability to print a sensitive document from RDINet. The SSCI staff member attempted to bypass the print restriction by reviewed the incident and recommended removing the possibility of SSCI staffers utilizing but because the capability was it could not be removed or disabled. The RDI team discussed this issue with SSCI staff and reminded them of the need for security of sensitive documents.[18]

[17](U) Ibid. ¶ 3.

[18](U) Ibid.

APPROVED FOR RELEASE DATE: 14-Jan-2015

II. (U) Events of Days in Question, January 2014

(U~~//FOUO)~~ Agency personnel searched the SSCI-side of RDINet or reviewed SSCI-related [redacted] over several days in January 2014. The Board grouped these activities into three separate "looks."

(U~~//FOUO)~~ [redacted] told the IG [redacted] ordered what the Board calls the first and second looks because [redacted] believed there was a security breach on RDINet. [redacted] suspected that privileged Weekly Case Reports (WCRs) could be on the SSCI's side of RDINet and had been accessed by SSCI staff.[19] [redacted] formed this belief because of a November 2013 Senate request for a copy of the "Panetta Review"; because a draft SSCI report contained language remarkably similar to portions of the "Panetta Review"; and because of a statement by a SSCI staffer that the staffer had "seen the real response."[20]

(U) The First Look

(U~~//FOUO)~~ On or about 9 January, [redacted] instructed [redacted] to search RDINet to determine whether particular Agency-created documents not yet cleared for transfer were resident on the SSCI accessible portion of the database.[21] Specifically, [redacted] wanted to know whether the privileged and deliberative draft CIA summary documents known variously as the "Panetta Review," "Special Review Team Documents (SRT)," or WCRs" were inappropriately on the SSCI side of the database.[22] RDI personnel conducted this look on or about 9 and 10 January 2014. [redacted] has maintained that the Agency's obligations under the National Security Act created a

[19] (U~~//FOUO)~~ OIG notes of 27 March 2014 [redacted] Interview, ¶ 7 and 15.

[20] (U) Ibid. ¶¶ 7-10, 13.

[21] (U~~//FOUO)~~ OIG notes of 27 March 2014 [redacted] interview, ¶ 15.

[22] (U) Ibid. ¶ 8.

APPROVED FOR RELEASE DATE: 14-Jan-2015

legal duty to search the SSCI side of RDINet for the presence of Agency documents to which SSCI staff should not have access.[23]

(U~~//FOUO~~) The [redacted] RDINet IT employee, [redacted] recalls being instructed by [redacted] on 9 January 2014 to conduct searches of RDINet for the presence of files with "WCR" or "SRT" in their titles.[24] First, [redacted] searched the database containing documents to which the Agency had granted SSCI access[25] and no file with WCR or SRT in its name was present on that portion of RDINet.[26] Next, [redacted] conducted a Google search of RDINet, which by virtue of [redacted] administrator access, searched the entirety of the network.[27] That search disclosed as expected that WCR and SRT files resided on the CIA side of the network, but also that they were present on the SSCI Majority Staff user drive.[28] Finally, [redacted] conducted a root search with the search terms WCR and SRT, which revealed that files with those names were located on one SSCI Majority Staff user drive, and the SSCI Majority shared drive.[29]

(U~~//FOUO~~) When questioned by the IG, [redacted] recalled instructing [redacted] on 10 January to demonstrate how SSCI staff would have looked at the WCR documents on the SSCI side of the network.[30] [redacted] recalled asking [redacted] to help [redacted] take screenshots of the Majority share drive folder and subfolder in which the WCR documents resided, and to demonstrate how SSCI staff could use the Google appliance to locate the documents.[31] [redacted] said [redacted]

---

[23] (U~~//FOUO~~) [redacted] AAB Submission, p. 6.

[24] (U~~//FOUO~~) [redacted] AAB Submission, p. 2.

[25] (U) Ibid.

[26] (U) Ibid.

[27] (U) Ibid.

[28] (U) Ibid.

[29] (U) Ibid.

[30] (U~~//FOUO~~) OIG Notes of 22 April 2014 [redacted] OIG interview, ¶ 22.

APPROVED FOR RELEASE DATE: 14-Jan-2015

did not recall whether this required [redacted] to adjust [redacted] network permissions.[32]

(U~~//FOUO)~~ There is no evidence that any SSCI work product—e-mails, drafts, or other confidential or deliberative material of any type—were accessed at that time.

~~(C//NF)~~ There is disagreement about the timing of the activity [redacted] recalls as occurring on 9 January, and who participated in the activity. The OIG concluded that [redacted] assisted [redacted] on the 9th,[33] but time and attendance records show [redacted] on leave that day[34] and [redacted] recalled assisting [redacted] on the 9th.[35] [redacted] recalls the RDINet searches being conducted between 6 and 8 January, not 9 and 10.[36] [redacted] recalled that [redacted] had determined that SSCI staff had access to the WCR documents on 7 or 8 January.[37] The OIG Report also says [redacted] opened "a few" of the files on the 9th,[38] but that finding is not corroborated by the OIG interview notes or the various AAB submissions. [redacted] surmises that the OIG confused the activities of the 9th with activities of the 10th.[39]

---

[31](U) Ibid.

[32](U) Ibid. ¶ 23.

[33](U) OIG Report ¶ 24.

[34]~~(C//NF)~~ [redacted] AAB Submission, p. 9 and Exhibit 3.

[35](U~~//FOUO)~~ [redacted] AAB Submission, p. 2.

[36]~~(C//NF)~~ [redacted] AAB Submission, p. 6

[37](U~~//FOUO)~~ OIG Notes of 27 March 2014 [redacted] OIG Interview, ¶ 14.

[38](U) OIG Report ¶ 24.

[39](U~~//FOUO)~~ [redacted] AAB Submission, p. 2.

APPROVED FOR RELEASE DATE: 14-Jan-2015

(U) The Second Look

(U~~//FOUO~~) The second look commenced on or about 10 January, when [redacted] attempted to learn whether SSCI Staffers had actually accessed or printed the WCR documents.[40] If the documents had not been accessed or copied, the potential security concerns and need to approach SSCI would be more limited. [redacted] stated in [redacted] IG interview that [redacted] reported the results of the first look to the [redacted] and the [redacted] on the 9th,[41] and that "between [redacted] (the [redacted]), and [redacted], they decided to approach the next step as determining whether the files had been accessed by SSCI."[42] [redacted] recollection of this meeting is consistent with the [redacted][43]

~~(S//NF)~~ [redacted] did this by asking [redacted] to task CIC [redacted], which [redacted] believed to be [redacted][44]

(U~~//FOUO~~) In [redacted] statement, [redacted] says that the [redacted] visited [redacted] on 9 January after briefing the D/CIA about the results of "the first look," and conveyed an explicit instruction to [redacted] that [redacted] determine whether SSCI staff had accessed or printed the documents.[45] Specifically, [redacted] recalled being told by the [redacted] that the D/CIA "wanted to be 'completely sure' that the documents were, in fact, what they appeared to be . . . and also wanted to know if they had been printed, as he was concerned the documents could have been

---

[40](U) Ibid. ¶ 20.

[41](U) Ibid. ¶ 15.

[42](U) Ibid. ¶ 17.

[43](U~~//FOUO~~) AAB 14 October 2014 [redacted] Interview (When I heard about this, I thought the facts were not correctly developed. I wanted to know of the WCRs were just sitting there, or had they been used, or were taken. If they were accessed, how often and by whom?)

[44](U~~//FOUO~~) OIG notes of 27 March 2014 [redacted] interview, ¶ 17.

[45](U~~//FOUO~~) [redacted] AAB Submission, p. 10.

APPROVED FOR RELEASE DATE: 14-Jan-2015

secretly removed from the CIA facility."[46] [redacted] also wrote in [redacted] statement that the D/CIA himself reiterated these explicit instructions to [redacted] on three occasions between 10 and 13 January.[47]

(U~~//FOUO)~~ A misunderstanding between the D/CIA and [redacted] arose because the former did not appreciate what forensic techniques were necessary to answer his questions and the latter did not understand the D/CIA's expectations that no intrusive methods be employed.

~~(S//~~[redacted]~~NF)~~ On 10 January 2014, [redacted] sought to determine whether SSCI users accessed the WCR documents by tasking [redacted] to [redacted] who accessed documents contained in [redacted] folder of RDI Net for the period 3/1/2009 to 12/31/2013."[48] In a follow-on tasking, [redacted] for the same documents . . . to determine whether staffers would have had the opportunity to take the documents for the Hill in hard copy."[49]

~~(S//NF)~~ In addition to describing the information sought, the [redacted] tasking expressly limited where [redacted] was to look. [redacted] first e-mail to [redacted] carried the following caveat:

> We ask that you provide us ONLY the [redacted] documents in this folder and its component sub-

---

[46](U) Ibid.

[47](U~~//FOUO)~~ Ibid. pp. 10-11 ("First in his office on the night of January 10; second during a call placed to me at home on the afternoon of January 11; and third, in a passing conversation in the doorway of his office on January 13. In the January 11 call, the D/CIA particularly emphasized his desire to confront SSCI leadership immediately with information concerning the matter. As a predicate to doing so, however, he felt the need to have a clear understanding of how the documents came to be accessible by SSCI Staff.")

[48]~~(S//NF)~~ [redacted] AAB Submission, tab 1, 10 January 2014 (09:18 AM) e-mail from [redacted] to [redacted] staff.

[49](U~~//FOUO)~~ 10 January 2014 (07:25 PM) e-mail from [redacted] to CIC [redacted] advisors.

folders. Please **DO NOT** undertake this tasking if it would require that you search and/or provide us [redacted] relating to other contents of the RDI Net Y: drive, as this drive is a SSCI staff drive on the RDI Net system.[50]

~~(S//NF)~~ After [redacted] follow-on tasking, [redacted] repeated this caveat in an e-mail to CIC [redacted] on 13 January 2014,[51] "To follow up on our conversation this morning, please be sure that CIC [redacted] understands that the scope of the documents under review has not/not changed. [redacted] should be told expressly to look ONLY at the provenance of the documents in the [redacted]

(U~~//FOUO~~) [redacted] reiterated the caveat: "I can't stress how important this is. We need to confine this review as narrowly as possible, and make sure everyone understands this is not a fishing expedition into SSCI files (emphasis added)."[52]

(U~~//FOUO~~) When the Executive Director convened a meeting with senior Agency leadership on the morning of 14 January, each person present was either aware of the first and second looks and approved of the action [redacted] had taken to date, or posed no objection.[53, 54, 55, 56] the CIC [redacted] also was present at the

---

[50] ~~(S//NF)~~ [redacted] AAB Submission, tab 1, 10 January 2014 (09:18 AM) e-mail from [redacted] to [redacted] staff (emphasis in original).

[51] ~~(S//NF)~~ [redacted] AAB Submission, tab 3, 13 January 2014 (09:18 AM) e-mail from [redacted] to CIC [redacted]

[52] ~~(S//NF)~~ [redacted] AAB Submission, tab 3, 13 January 2014 (04:57 PM) e-mail from [redacted] to CIC [redacted]

[53] (U~~//FOUO~~) OIG notes of 9 April 2014 EXDIR interview, ¶ 10 (meeting attendees surprised by the D/CIA's decision not to learn how the documents got on the SSCI side and felt that Agency personnel had not exceeded their authority or acted inappropriately regarding the review of RDI events.)

[54] (U~~//FOUO~~) OIG notes of 15 April 2014 the [redacted] interview, ¶ 16 ("he knew [redacted] was having [redacted] IT guys look at it. . . [and] [redacted] actions did not strike him as problematic or in any way untoward").

[55] (U~~//FOUO~~) OIG notes of 2 April 2014 the [redacted] interview, ¶ 18 ("SSCI had documents on their side that were not passed through the firewall. According to the [redacted] all of the information was provided by [redacted] and

APPROVED FOR RELEASE DATE: 14-Jan-2015

meeting and recalled that the "[redacted] repeatedly emphasized that the 'D/CIA wants to GO' on this issue."[57]

(U) The Third Look

(U~~//FOUO~~) The third look, while benign in intent, was characterized by miscommunications, is the source of greatest controversy, and raised the most questions about the scope of the Agency's security review.

~~(S//NF)~~ [redacted] and the Office of Security's Cyber Blue Team (CBT) conducted this third look. [redacted] analyzed activity on the SSCI folder containing the WCRs to determine if any documents were printed from that folder and how the WCR's got onto the SSCI side of RDINet.[58] The CBT review was conducted to determine how SSCI could have gained access to the WCRs, how a SSCI user could discover the WCRs, and how the Agency knew that SSCI acquired access to the WCRs.[59] The Board tried to piece together the communications used to start, stop, modify, and continue these activities.

~~(TS//~~[redacted]~~//NF)~~ In his OIG interview, a [redacted] contractor employee explained that he was tasked "sometime in January 2014" with [redacted] on RDINet, and specifically, the "CIA side."[60] He was

---

[redacted] The [redacted] stated that they knew the files were there through whatever computer action had taken place. He stated that he did not understand fully how they found them.")

[56] (U~~//FOUO~~) [redacted] AAB Submission, p. 8. (Also present at the EXDIR meeting the morning of 14 January were the [redacted] Acting General Counsel, Director of the Office of Public Affairs, Director of the Office of Congressional Affairs, [redacted] the Counterintelligence Center (CIC), [redacted] [redacted] CIC, [redacted] to the EXDIR.) No one raised an objection to [redacted] actions.

[57] ~~(S//NF)~~ Timeline provided by [redacted] CIC during AAB Interview.

[58] ~~(S//NF)~~ OIG notes of 11 March 2014 [redacted] contractor interview, ¶ 2.

[59] (U~~//FOUO~~) OIG notes of 20 March 2014 CBT [redacted] interview, ¶ 4.

[60] ~~(S//NF)~~ OIG Notes of 12 March 2014 separate [redacted] contractor, ¶ 3.

APPROVED FOR RELEASE DATE: 14-Jan-2015

investigating the possibility that the documents were provided to the SSCI staff by a leaker though "HUMINT."[61] The [redacted] contractor did not have access to the RDINet hard drives, network share drives, or actual RDINet files.[62] Rather, he looked "at [redacted] that had previously been collected by [redacted] as part of 'normal CIA [redacted] on CIA networks.'"[63] The [redacted] contractor explained that, for RDINet, [redacted][64] He found no evidence of a HUMINT leak, and theorized that a misconfiguration of the google appliance may have given SSCI staff access to the document.[65] However, a stand down order from the Director, discussed below, arrived before he could test that theory.[66]

(U~~//FOUO)~~ When the D/CIA was briefed the evening of 14 January 2014 about the foregoing, he ordered the stand down.[67] He then proposed a joint CIA-SSCI review of the matter,[68] which the SSCI shortly thereafter declined to participate in.[69] At no time did the D/CIA order any further forensic work to be undertaken.[70]

~~(S//NF)~~ Upon returning from that evening's meeting with the D/CIA, [redacted] CIC instructed [redacted] "to 'stand down immediately' on any tasking on this issue."[71] Those working the issue had

---

[61](U) Ibid.

[62](U) Ibid.

[63](U) Ibid.

[64](U) Ibid., ¶ 7.

[65](U) Ibid., ¶ 8.

[66](U) Ibid.

[67](U//FOUO) OIG Notes of 21 April 2014 D/CIA OIG Interview, ¶ 6.

[68](U//FOUO) Ibid., ¶ 8.

[69](U) Ibid., ¶ 10.

[70](U) Ibid., ¶ 9.

[71](U~~//FOUO)~~ Timeline provided by [redacted] CIC during AAB Interview.

APPROVED FOR RELEASE DATE: 14-Jan-2015

departed for the day, and eventually, CIC was reached at home and instructed to call CIC at home with the order to instruct the two contractor analysts to stand down immediately.[72]

(U~~//FOUO~~) After the D/CIA briefing, the contacted the the Office of Security OS) at home about the proposed joint review .[73] The asked OS if the OS could lead an investigation of an IT issue.[74] called OS 15 minutes later and said the issue would be discussed at work on 15 January.[75] The SSCI Security then called and explained the work would be part of a joint SSCI-CIA review.[76]

~~(S//NF)~~ CIC's stand-down order apparently was not delivered in a timely fashion. According to one contractor employee, he was ordered on 15 and 16 January by the to look into that was available for RDINet.[77] There were three tasks: 1) analyze activity on the specified folder; 2) determine and, 3) determine the provenance of the documents.[78]

~~(S//NF)~~ On 15 January, several Agency officers met to scope the OS review and effect the turnover from to OS.[79] OS understood the guidance from the 14 January D/CIA meeting was

---

[72] (U) Ibid.

[73] (U~~//FOUO~~) OIG Notes of 3 April 2014 OIG Interview, ¶ 30.

[74] (U~~//FOUO~~) AAB Notes of 8 September 2014 OS Interview, p. 1.

[75] (U) Ibid.

[76] (U) Ibid.

[77] ~~(S//NF)~~ OIG notes of 11 March 2014 contractor employee Interview, ¶ 2.

[78] (U) Ibid.

[79] ~~(S//NF)~~ Ibid. In attendance were OS, CIC, CIC OS Officer, and OGC attorneys and CIC

APPROVED FOR RELEASE DATE: 14-Jan-2015

that CIC would stop its work and that OS would look at [redacted] to determine if a violation occurred.[80] (S//NF) At a meeting also on the 15th [redacted] the Cyber Blue Team (CBT) received a tasking from [redacted] and [redacted] OS.[81] The oral tasking was followed by an e-mail confirmation.[82] The CBT was ordered to review the [redacted] data to determine how SSCI could have gained access to the restricted documents.[83]

~~(S//NF)~~ A [redacted] contractor employee was assigned to help the Office of Security's Cyber Blue Team (CBT) conduct its review.[84] He stated that the CBT's tasks were to verify that unauthorized documents were in a specific location, and if so determine how they got there.[85] According to the employee, the combined team concluded that someone directly navigate to the file path containing the unauthorized documents and copied them to another SSCI accessible location.[86] However, he was unsure of how that individual discovered the folder path that led him or her to the documents.[87]

~~(S//NF)~~ When interviewed by the OIG, [redacted] said the first tasking from [redacted] OS called for a full forensic review of the SSCI systems.[88] However, before CBT accessed any part of the SSCI side of RDINet, [redacted] OS countermanded that order and limited CBT's

---

[80] (U~~//FOUO~~) AAB Notes of Interview with [redacted] OS p.2.

[81] (U~~//FOUO~~) OIG notes of 20 March 2014 [redacted] Cyber Blue Team Interview, ¶ 4.

[82] (U) Ibid.

[83] (U) Ibid.

[84] ~~(S//NF)~~ OIG Notes of 11 March 2014 Interview of [redacted] contractor employee, ¶ 3.

[85] (U) Ibid.

[86] (U) Ibid.

[87] (U) Ibid.

[88] (U~~//FOUO~~) OIG Notes of 13 March 2014 Interview of [redacted] ¶ 2.

APPROVED FOR RELEASE DATE: 14-Jan-2015

review to the [redacted] monitoring of RDINet.[89]

(U~~//FOUO~~) When interviewed by the OIG, a CBT analyst said their review identified by name the SSCI user responsible for originally accessing the unauthorized documents.[90] The SSCI employee accessed at least 166 files. The review also discovered that beginning on November 9, 2010 the restricted documents were later disseminated among four other SSCI staffers and printed.[91] The names of the SSCI staffers were removed from the final CBT report and replaced with IDENs.[92]

(U~~//FOUO~~) Although OIG interview notes mention the CBT's conclusions, they do not describe the facts on which the CBT based its conclusions. The OIG Report's Executive Summary says the CBT report contains some "forensically reconstructed" SSCI staffer e-mails.[93] And the body of the OIG Report describes those e-mails as "communication between 'Congressional users' that directed them to review specific documents."[94] As previously indicated, SSCI communications inappropriately reviewed by Agency staff were limited in number (five) and did not involve discussions of substantive matters in content. The CBT report lists five e-mails made by one staffer:

[redacted]

---

[89](U) Ibid.

[90](U~~//FOUO~~) OIG Notes of 13 March 2014 CBT analyst Interview, ¶ 3.

[91](U) Ibid.

[92](U~~//FOUO~~) OIG Notes of [redacted] Interview, ¶ 2.

[93](U) IG Report, Executive Summary, p. iii.

[94](U) IG Report, p. 44.

APPROVED FOR RELEASE DATE: 14-Jan-2015

[redacted]

~~(S//NF)~~ The OIG found that [redacted] OS ordered the CBT review under [redacted] own authority as a normal OS function and did not believe [redacted] needed to seek higher approval.[95] [redacted] OS believed [redacted] actions were consistent with the D/CIA's stand down order because [redacted] thought it applied to the joint CIA-SSCI investigation, not to an internal review of [redacted] already had compiled.[96]

(U~~//FOUO)~~ This third look resulted in inappropriate access to SSCI work product. While the access was limited—a total of five e-mails, none of any consequence or involving discussions of substantive matters—it was inconsistent with the D/CIA stand-down order and with the work product limitations emphasized by [redacted] and [redacted] in their taskings.

III. (U) The OIG Findings: Questions and Issues of Fact

A. (U) Undisputed Facts

(U~~//FOUO)~~ The Agency and SSCI did not enter into a signed, final agreement to govern the management of security in this unusual circumstance, but agreed to resolve issues informally, case by case. No record exists to establish that the SSCI staff security briefings agreed to in principle were provided.

(U~~//FOUO)~~ The Agency monitored and collected all computer activity on RDINet as part of its standard information system

[95](U) IG Report, p. 43.

[96](U) Ibid.

APPROVED FOR RELEASE DATE: 14-Jan-2015

security process. The [redacted] included all activity on the SSCI portion of the network.

(U~~//FOUO)~~ On the basis of this monitoring, and as known by SSCI staff, previous instances of improper conduct on the RDINet had been identified and responsive security measures taken. On certain occasions, SSCI staff requested CIA technology staff assistance in locating documents by accessing SSCI space on the system.

(U~~//FOUO)~~ [redacted] in discussions with [redacted] made the decision to find out if SSCI staff had access to WCR or SRT documents that were deemed privileged, and not part of the SSCI review, and were created after the information cut-off date of 22 January 2009.

(U~~//FOUO)~~ [redacted] directed RDINet IT officers to help [redacted] determine the location of the WCRs and SRTs on RDINet and the documents were discovered on the SSCI portion of the shared drive.

~~(S//NF)~~ CIC [redacted] was brought in to examine its [redacted] to determine if SSCI staff accessed and used the WCRs and SRTs.

~~(S//NF)~~ The Office of Security's Cyber Blue Team analyzed [redacted] and the Team's final report included a limited number of SSCI staff e-mails.

B. (U) Facts and Issues in Dispute

1. (U) Legal Authorities and Authorization

(U~~//FOUO)~~ The IG concluded that communications in 2009 between SSCI and the Agency created a common understanding that CIA access to the SSCI portion of RDINet would be restricted to IT staff for administrative purposes unless authorized by the SSCI. In this context, the IG found actions directed or performed by [redacted] and the IT staff to be improper and/or unauthorized.

(U~~//FOUO)~~ IG investigators highlighted to the Board that the five officers were not part of an investigative body (CIC, OS,

or OIG) and had no investigative authority. Two IG officers had extensive IT experience and further noted to the Board that actions taken by the IT officers were unusual and beyond what is expected for an IT officer.

(U~~//FOUO)~~ The five officers countered the IG's findings by highlighting how searches for documents on RDINet had become a common practice over the years with IT staff regularly called upon to help determine the location of documents across RDINet. They also emphasized that the Agency always maintained responsibility for RDINet security, and the SSCI was aware of this fact from previous incidents and express notification before access to the system. With respect to who should have initiated an investigation, [redacted] determined [redacted] had the authority and responsibility to ensure the security of RDINet and [redacted] actions were in line with [redacted] responsibilities. In [redacted] written response to the IG report, [redacted] notes that the System Security Plan [redacted] to address unauthorized access.

(U~~//FOUO)~~ The Board notes that [redacted] proactively and consistently communicated that the Agency take very limited actions so it would not intrude upon SSCI work product.

2. (U) Accountability and Reporting to Leadership

(U~~//FOUO)~~ There is some confusion as to who in Senior Leadership authorized what action and when they issued these directives. The OIG told the Board that [redacted] conveyed the D/CIA's interest in the matter before [redacted] had received feedback from the D/CIA, but other information before the Board makes it appear there was regular dialogue with leadership as events unfolded. Alerts to the D/CIA can take different paths and it appears that the Acting General Counsel, the [redacted] and the [redacted] were informed of the discoveries after the first look. Of note, it was difficult for the Board to develop a precise timeline because events happened in parallel and some of the communications were face-to-face or via phone calls.

APPROVED FOR RELEASE DATE: 14-Jan-2015

3. (U) Recusal Question

(U~~//FOUO~~) The IG report notes that the Acting General Counsel by 7 February 2014 had previously recused himself from RDI-related matters and was therefore unaware of programmatic details. The IG asserts that the recusal meant [redacted] did not have a supervisor during the events in question.

(U~~//FOUO~~) When interviewed by the Board on 8 September 2014, the Acting General Counsel explained that he recused himself after the 11 March 2014 SSCI Chair speech on the Senate floor and was not recused when he signed out the crimes report on 7 February 2014. He explained his active participation throughout the events in question and that he had a discussion with [redacted] about the potential security incident where he outlined the key issues as:

- RDINet is an Agency system.
- SSCI staff members were briefed on the audit capability (the Board could not confirm SSCI staffers were briefed on this audit capability).
- IT staff had authorized access.
- There was a past practice of removing items from the SSCI side of RDINet.
- That it is within Agency responsibilities to determine if someone took something.

IV. (U) Board Conclusions

A. (U) Standard for Reviewing Conduct

(U~~//FOUO~~) The Board determined there was no agreement between SSCI and the Agency on what steps would be taken in the event of a suspected security incident. In the absence of an agreement, the Agency followed its standard security practices with the understanding that the separations of powers concerns were very sensitive, and of keen importance to Agency leadership, and that SSCI work product should, therefore, be protected.

(U~~//FOUO~~) In the absence of a formal agreement, the Board the "reasonable person" standard when evaluating the actions of the five individuals. The Board notes that this is the standard that

APPROVED FOR RELEASE DATE: 14-Jan-2015

the OIG told the Board was used in evaluating the conduct in question.

(U~~//FOUO~~) The Board did not attempt to define what path, decisions, or courses of action would represent the most reasonable responses among various reasonable alternatives, but instead evaluated if the conduct of these officers could be determined to have been unreasonable.

(U~~//FOUO~~) Under the "reasonable person" standard, it is possible that different conclusions can be reached by different people from the same set of facts. This is particularly so in a fundamentally complex case such as this, involving an unprecedented shared system holding millions of highly sensitive materials which was operated by the Agency and the Senate without a clear, settled agreement on the management of security.

(U~~//FOUO~~) The fact that the potential security breach involved a co-equal branch of the United States Government added substantially to the complexity and sensitivity of the situation. Great certitude was understandably desired before raising it with the Senate and pursuing formal allegations of wrongdoing.

B. (U) Legal Authorities and Authorization

(U) Application of Criminal Law § 1030

(U~~//FOUO~~) The IG referred this matter to the Department of Justice for potential violations of the Wiretap Act and the Computer Fraud and Abuse Act.[97] The OIG Report provided no rationale for either referral. In Board interviews, the investigative staff asserted that [redacted] violated the Computer Fraud and Abuse Act because they accessed the SSCI side of RDINet in violation of an unwritten "Common Understanding" between CIA and the SSCI.

(U~~//FOUO~~) The facts and circumstances of this case do not support the use of either statute to establish "unauthorized access" by these Agency personnel. The Wiretap Act criminalizes

[97] (U) IG Report, ¶ 1.

APPROVED FOR RELEASE DATE: 14-Jan-2015

under certain circumstances the intentional interception, disclosure, or use of the electronic communications of others. 18 U.S.C. § 2511. The Act excludes from its coverage the interception of electronic communications if a party consents to the interception. Id. § 2511(2)(c). Each time a SSCI staffer logged onto RDINet, he or she was presented with the warning that his or her actions were subject to monitoring, and asked to consent to the monitoring as a condition of accessing the system. Thus, SSCI Staffers consented to Agency access of the SSCI side of RDINet for some purposes, not to include the examination of SSCI work product. The Act also excludes from its coverage the interception of communications "under color of law to intercept the . . . communications of a computer trespasser." Id. § 2511(i). When Agency personnel accessed information from the SSCI Side of RDINet, they were investigating suspected access to highly classified information from the CIA side of RDINet, which the Agency has a legal duty to protect from unauthorized disclosure. Accordingly, the Wiretap Act does not support a finding of Agency personnel misconduct in the relation to the events of January 2014.

(U~~//FOUO)~~ There also is no basis for such a finding in the Computer Fraud and Abuse Act referral. An individual violates that Act when he "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains - . . . Information from any department or agency of the United States." 18 U.S.C. § 1030(a)(2)(B). The Board could not find evidence of a "Common Understanding" that would have prevented [redacted] from looking on the SSCI side of RDINet for the presence of CIA documents—highly classified and sensitive documents SSCI was not entitled to access. To the contrary, CIA routinely and without controversy searched the SSCI side of RDINet for CIA documents and it did so on certain occasions at SSCI staff request.

~~(S//NF)~~ As for the more detailed examination conducted by [redacted] at [redacted] direction, [redacted] reasonably believed [redacted] was acting under the authority of the D/CIA when [redacted] tasked [redacted] to discover whether SSCI staff had accessed and printed the documents.

APPROVED FOR RELEASE DATE: 14-Jan-2015

(U~~//FOUO~~) Because there is no basis for a finding against [redacted] under these statutes, neither can they establish misconduct [redacted] who simply carried out [redacted] instructions.

C. (U~~//FOUO~~) The Reasonableness of [redacted] and [redacted] Actions

(U~~//FOUO~~) As previously noted, by early January 2014 [redacted] had reason to believe that CIA documents had been accessed without authorization by SSCI staff. The origins and extent of the probable security breach were unknown to [redacted]

(U~~//FOUO~~) This presented [redacted] with a dilemma. [redacted] needed to ensure that a CIA system containing substantial sensitive material was secure. [redacted] also needed to safeguard the prerogatives of the Senate, particularly the protection of work product.

(U~~//FOUO~~) Several courses of actions were possible, but none were without risk. In fact, no good options may have existed and any may have led to the subsequent controversy.

(U~~//FOUO~~) [redacted] chose to first verify that a security breach in fact existed before informing [redacted] superiors. This seems reasonable given the embarrassment to the Agency and harm to the Agency-SSCI relationship that would have resulted from a false allegation. [redacted] at all times attempted to limit the scope of the verification process. On the day the document was discovered on the SSCI side of the RDINet, [redacted] relayed this information to Agency leadership. There is no evidence that [redacted] authorized the review of SSCI work product.

~~(S//NF)~~ The IG contends that [redacted] should not have undertaken steps to verify [redacted] concerns and instead should have gone to the Office of Security. This would have spared [redacted] adverse OIG findings, but in all likelihood could have led to the same controversy or worse. [redacted]

[redacted]

APPROVED FOR RELEASE DATE: 14-Jan-2015

[redacted]

(U~~//FOUO~~) [redacted] subsequent efforts to determine whether the documents had been copied or accessed also seem reasonable. First, [redacted] understood the D/CIA to have requested that [redacted] do so (even though the D/CIA did not fully appreciate the technical methods this effort would necessitate). Second, this was no normal potential security problem; it involved the United States Senate. Accordingly, it seems reasonable for [redacted] to have explored all alternatives and possible solutions before the problem was confirmed and the D/CIA would have raised it with Senate leaders.

(U~~//FOUO~~) The Board evaluated [redacted] actions in light of directives [redacted] received from [redacted] to determine the presence of documents on the SSCI side of RDINet. The Board considered [redacted] actions to use IT permissions to search for the documents as arguably unorthodox, but they seemed to be within reason given the imperative relayed to [redacted] by [redacted]

~~(S//NF)~~ In [redacted] written statement to the Board, [redacted] highlighted the Agency on 8 January 2014 responded to the 26 November 2013 SSCI request for copies of the "Panetta Review and associated materials" after the White House Counsel's office reviewed them on 7 January 2014 and confirmed they were subject to privilege. This sets the framework for [redacted] initial speculative discussions with [redacted] that SSCI staffers likely had access to the documents. [redacted] had a lingering concern with the Google search tool configuration because SSCI staffers in April 2013 obtained a copy of a privileged spreadsheet containing a list of Agency videos and the staffers agreed with the Agency to destroy the document.[98]

~~(S//NF)~~ Regarding the use of SSCI-like access, [redacted] wrote to the Board that "we sought to test whether the previously known Google misconfiguration still existed and allowed an IT professional with IT permissions of a SSCI user to access particular nonresponsive, privileged **CIA** documents, which existed on RDINet with restrictions intended to limit access only to CIA users." (emphasis in the original) Search terms were

[98] (U~~//FOUO~~) [redacted] AAB submission, pages 9-10.

APPROVED FOR RELEASE DATE: 14-Jan-2015

chosen to return only CIA work product and [redacted] first assumption was SSCI staff could have accessed the documents in a CIA-only location. [redacted] was surprised to see the documents "saved into a space intended for SSCI work product."[99]

(U~~//FOUO)~~ [redacted] briefed [redacted] actions to Agency leaders at the previously mentioned 14 January 2014 morning meeting and none of the officers present objected to the way [redacted] identified the documents. Upon the D/CIA's later stand down directive, [redacted] wrote to the IT staff to see if access to the documents could be restricted but directed that no further steps be taken.[100]

(U~~//FOUO)~~ Summary: It is entirely possible that reasonable people would make different decisions under this complex, unique set of circumstances. We conclude, however, that [redacted] and [redacted] did not act unreasonably and in fact tried to carefully balance both need for RDINet security with the desire to protect SSCI work product while ascertaining the facts necessary for their superiors' review.

D. (U) Candor (IT staff)

(U~~//FOUO)~~ The IG findings of lack of candor against the IT employees did not assert untruthfulness. Instead the IG contends that their responses were initially incomplete and that reasonable persons would have highlighted their actions taken at the direction of the OGC officers.

(U~~//FOUO)~~ This contention is unsupported for numerous reasons. First, no transcript, recording, or other comprehensive record of the interviews exists, so it is impossible to reconstruct the questions asked of the IT employees and their purportedly evasive answers.[101] Second, the purported problematic responses

---

[99] (U) Ibid, page 10.

[100] (U) Ibid, page 13.

[101] ~~(C//NF)~~ The Board notes that in the IG's Memorandum of Investigative Activity (MOIA) that summarizes their only interview with [redacted] on 4 February 2014, paragraph 8 quotes [redacted] on [redacted] participation in a meeting with [redacted] approximately three weeks prior to the interview. The Board assumed this meeting was related to the events in question and [redacted] might have intended to have referred to them.

APPROVED FOR RELEASE
DATE: 14-Jan-2015

came at the end of very brief interviews which focused mostly on unrelated technical matters, so there is a reasonable basis for the IT employees' belief that they were being responsive. Third, the IG staff characterized the questions they asked as intentionally general and designed to elicit as broad a response as possible, not specific and detailed responses. Fourth, when the Board interviewed the IT employees, each credibly denied any attempt to evade questioning. Fifth, [redacted] and [redacted] were open about the searches they had ordered, so it would have been purposeless for the IT employees to conceal their actions.

(U~~//FOUO~~) The Board evaluated the OIG's questions used during their first interviews of the three IT officers and the Board as unable to discern questions that would have led [redacted] and [redacted] to explain their recent work under the direction of

(U~~//FOUO~~) IG investigators stressed to the Board that [redacted] and [redacted] provided relevant details when they were "confronted with the evidence." However, there is no evidence mentioned in the corresponding MOIAs, and the OIG did not document the exact content of the questions asked during the second interview. When pressed, one investigator could not recall what was shown during the interview.

(U~~//FOUO~~) Under these circumstances, where the alleged transgression is a lack of completeness not lying, more is needed to conclude that the individuals involved were unreasonable in their initial responses. The Board concluded that the allegations of lack of candor were unsupported by the evidence.

E. (U) Crimes Report Questions: Clarification In the Course of the IG Interviews

(U~~//FOUO~~) The IG asserted that [redacted] provided inaccurate information that was subsequently included in the 7 February 2014 letter to DOJ. The OIG in interviews with the Board stated the OIG did not intend to suggest that [redacted] acted improperly in providing this information. The Board determined that this assertion is at any rate erroneous. The

APPROVED FOR RELEASE
DATE: 14-Jan-2015

Cyber Blue Team provided the factual basis for the referral, wholly apart from any contribution by [redacted]

F. (U) In Extraordinary Circumstances, Difficulties with All Choices Available

(U~~//FOUO~~) The Board noted the difficulty of identifying the most appropriate, reasonable proper course of action for this security incident because nearly every such course is open to objection or question:

- (U~~//FOUO~~) The Agency agreed to hold work product as off-limits, yet was required to maintain the security of its network by installing [redacted] monitoring systems that saved nearly all computer events on the SSCI portion of RDINet.
- (U~~//FOUO~~) The common agreement called for a walled-off and stand-alone network but this was not implemented so documents could be easily shared with SSCI staff. Instead, access protocols were used to approve or deny access to each document in a common database and Agency IT staff had full view of the entire network.
- ~~(TS/~~ [redacted] ~~/NF)~~ [redacted] detected unauthorized activities on the SSCI portion of RDINet and these events documented that SSCI understood the extent of monitoring applied to the network. However, the OIG never located SSCI staff signed non-disclosure agreements that would verify their knowledge and acceptance of the security agreement.
- (U~~//FOUO~~) The Board was not presented with an instruction or guidance that described what would constitute the transfer of ownership for an Agency document. The Agency retrieved documents given to SSCI in error and SSCI staff complained this violated the (unsigned) agreement. However, the Agency declined to return the documents en masse and reviewed them for privilege, while at the same time the White House agreed in communications with Senator Feinstein that these were matters that required careful, sensitive treatment.

APPROVED FOR RELEASE
DATE: 14-Jan-2015

V. (U) Recommendations

A. (U) Recommendations Addressing Specific Issues and Allegations in this Matter

~~(C//NF)~~ After examining the facts, the Board recommends no disciplinary actions are warranted for [redacted] The Board found the actions and decisions of these officers to be reasonable in light of their responsibilities to manage an unprecedented computer system. The ambiguity surrounding the agreement between the SSCI and the Agency could have created alternative Agency responses and solutions to this potential security incident, but each could also have raised questions such as those giving rise to the OIG investigation and this Board review. The violation of SSCI work product that occurred resulted from communication failures, was not ordered by the individuals under review, and happened in spite of their protective efforts.

(U~~//FOUO~~) The Board has one recommendation that could improve how the Agency handles future potential security issues with Congress, and a separate recommendation for the Inspector General's consideration.

(U~~//FOUO~~) Recommendation 1: In any future questions of this kind involving Congress, advice from the Office of Congressional Affairs should be sought. Another assessment might not alter the course chosen but could lead to a more comprehensive evaluation of the matter and greater assurance that protective measures are in fact implemented in a manner less likely to generate conflict between the branches.

(U~~//FOUO~~) Recommendation 2: While the Board disagrees with the conclusions in the matter under review, we do not question that the OIG performs a valuable public service or that it did not strive to address appropriately the issues in this matter. It would better serve its investigative purposes, and aided this board in its review, if OIG kept more complete records of interviews.

APPROVED FOR RELEASE
DATE: 14-Jan-2015

B. (U) Systemic Recommendations

(U~~//FOUO~~) The Board found four systemic problems that surfaced in this matter and from which specific recommendations are offered.

(U~~//FOUO~~) Systemic Factor 1: No Signed Agreement and a Lack of Transparency between the SSCI and CIA Regarding RDINet

((U~~//FOUO~~)) As noted, the Board disagrees with the OIG that one could conclude there was a "common understanding" between the SSCI and CIA that would have governed the actions taken to determine the existence of a security incident. The core agreement was centered on the establishment of SSCI shared drives that would be walled-off but also accessible to CIA IT staff for the purpose of IT network administration.

- There was no documentation that established agreed-upon joint (SSCI and CIA) responsibilities and procedures to be used in the event of a suspected security incident.

- Several officers and the OIG highlighted that SSCI members clicked on the standard Agency warning banner when they logged onto RDINet and this warning included the text, "use of this system may be monitored and you have no expectation of privacy." However, SSCI staff members may not have been aware that standard monitoring capabilities included [redacted]

- SSCI work product was often cited as protected but these products were not clearly defined or agreed to by both parties.

APPROVED FOR RELEASE
DATE: 14-Jan-2015

(U//~~FOUO~~) Recommendation 3: For network connectivity involving two branches of government and/or multiple lines of authority, that the D/CIA direct the program's start-up and subsequent performance reviews include specific discussion and signed documentation by each stakeholder to include terms of references, network ownership, network monitoring roles and responsibilities, incident reporting, and accountability. The agreement shall be briefed to any officer involved with the effort and separate copies shall be kept in OIG, OS, and CIC.

(U//~~FOUO~~) Systemic Factor 2: Failure to Document and Update the RDINet Agreement in Light of Experience

(U//~~FOUO~~) The IG's investigation highlighted three incidents that could have served as watershed events to refine security restrictions for access to RDINet and further show how the Agency will rely on its monitoring capabilities to investigate breaches of security. The Board could not locate an updated agreement with the exception of a summary that directed Agency officers to consult with SSCI staff members before removing documents from the Reading Room. As previously mentioned:

- ~~(TS~~ [redacted] ~~NF)~~ In December 2009 the [redacted] monitoring [redacted] detected a SSCI Staff Member [redacted] Further analysis of monitoring data revealed the same Staff Member [redacted] on the network in November and December 2009 (though the OIG reported lists 2010) and the Member was removed from the team.

- (U//~~FOUO~~) In May 2010 the RDI team removed documents from the virtual reading room after they were unintentionally comingled with documents intended for the SSCI.

- ~~(TS~~ [redacted] ~~NF)~~ CIC [redacted] in May 2010 detected a Staff Member attempting to bypass a print restriction by [redacted] The RDI team reminded the SSCI staff of the need for security of sensitive documents.

APPROVED FOR RELEASE
DATE: 14-Jan-2015

(U~~//FOUO~~) Recommendation 4: For network connectivity involving two branches of government and/or multiple lines of authority, that the D/CIA direct a quarterly review for issues that may warrant clarification, policymaker awareness, notification, or further policy guidance.

(U) Systemic Factor 3: Authorities and Operations under One Hat

(U~~//FOUO~~) [redacted] created a situation where [redacted] fundamentally authorized [redacted] to investigate the potential security incident. Splitting these responsibilities would create shared responsibility and opportunities for discussion of alternatives and checks on matters of judgment.

(U~~//FOUO~~) Recommendation 5: If at all possible, the Agency should avoid assigning operational control and [redacted] oversight to one officer.

(U~~//FOUO~~) Systemic Factor 4: The Installation of a Computer Search Tool with Access Control Deficiencies

~~(S//NF)~~ The Agency installed a Google search capability at the request of SSCI staff members but the capability had vulnerabilities that provided SSCI staff with access to CIA protected documents. The search tool was installed as early as 2010 but was not fixed until April 2013.

(U~~//FOUO~~) Recommendation 6: For network connectivity involving two branches of government and/or multiple agencies, that the Office of Security address network security issues in a timely fashion and hold quarterly reviews for issues that may warrant clarification, notification, or further policy guidance.

C06274838

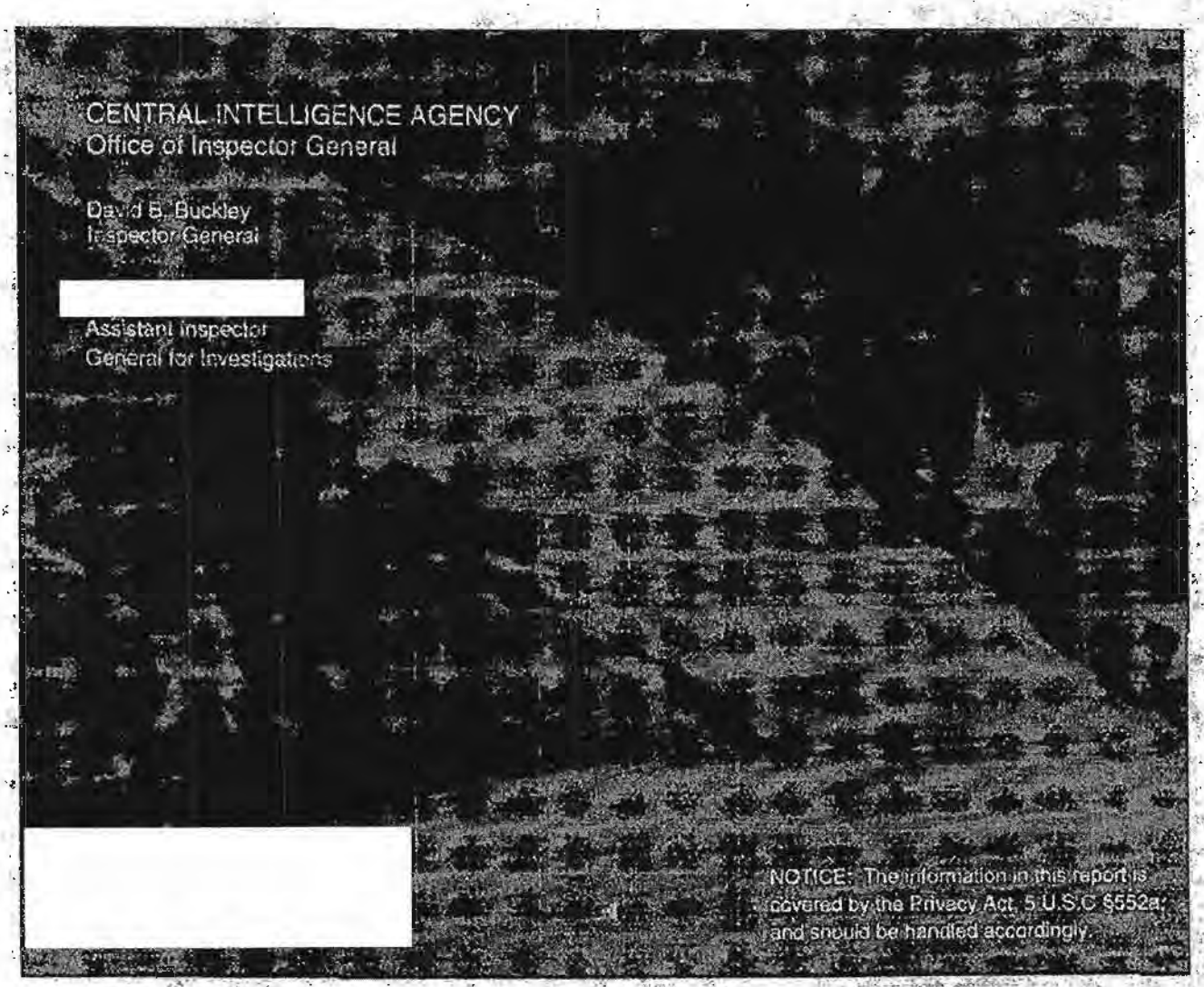
APPROVED FOR RELEASE DATE: 14-Jan-2015

~~SECRET//NOFORN~~

2014-11718-IG
18 July 2014

(U) REPORT OF INVESTIGATION

(U//FOUO) Agency Access to the SSCI Shared Drive on RDINet


CENTRAL INTELLIGENCE AGENCY
Office of Inspector General
David B. Buckley
Inspector General
Assistant Inspector
General for Investigations
NOTICE: The information in this report is covered by the Privacy Act, 5 U.S.C §552a; and should be handled accordingly.

~~SECRET//NOFORN~~

C06274838

APPROVED FOR RELEASE DATE: 14-Jan-2015

I. (U) Predication

1. (U//FOUO) On 29 January 2014, the Office of Inspector General (OIG) initiated a special review into the activities of CIA personnel related to the access of Senate Select Committee on Intelligence (SSCI) files and records on the Rendition, Detention, and Interrogation network (RDINet) located at the [redacted] building, an Agency facility in the [redacted] On 30 January 2014, OIG opened an investigation based on information discovered in the special review. In accordance with Title 50 U.S.C. § 3517, OIG reported the matter to the Department of Justice (DOJ) on 30 January 2014 for potential violations of Title 18 U.S.C. § 2511 (Wiretap Act) and 18 U.S.C. § 1030 (Computer Fraud and Abuse Act).

2. (U//FOUO) On 23 January 2014, SSCI Chairman Dianne Feinstein sent a letter to the Director, Central Intelligence Agency (D/CIA) John Brennan alleging that CIA personnel had "conducted one or more searches of the computer network at an offsite facility that the CIA had assigned exclusively to the staff of the [SSCI]." The letter detailed several questions Chairman Feinstein had regarding the conduct of CIA personnel and alleged violations of the 4th Amendment, the Speech and Debate Clause of the Constitution, the Computer Fraud and Abuse Act, and Executive Order 12333.

3. (U//FOUO) OIG investigation was limited to the alleged access of SSCI data on RDINet by Agency personnel (Exhibit A) in January 2014 and the subsequent actions taken. OIG investigation covered the issues of Agency personnel engaging in unauthorized access or exceeding authorized access to the RDINet, Agency monitoring of the RDINet, and whether a formal agreement had been made between the CIA and the SSCI regarding the use of RDINet. The activities of SSCI staff members were deliberately excluded from the investigation. No attempt was made to interview SSCI staff members, and digital forensics on RDINet and the associated [redacted] performed by OIG was limited in scope to avoid obtaining information related to the activities of SSCI users beyond that provided as part of the predication for the investigation. The U.S. Senate arranged for a specific review of the alleged misconduct by U.S. Senate staff to be conducted by the U.S. Senate Sergeant-at-Arms.

II. (U) POTENTIAL STATUTORY OR REGULATORY VIOLATION(S)

- *(U) Title 18 United States Code § 2511 Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited (Wiretap Act)*
- *(U) Title 18 United States Code § 1030 Fraud and Related Activity in Connection with Computers (Computer Fraud and Abuse Act)*

C06274838

APPROVED FOR RELEASE DATE: 14-Jan-2015

III. (U) BACKGROUND

(U) Review of the Rendition, Detention, and Interrogation Program

4. (U//FOUO) On 26 March 2009, the SSCI informed the CIA that the SSCI planned to conduct a thorough review of the CIA's RDI Program[1]. On 22 June 2009, the SSCI staff began their review. The review necessitated access by SSCI staff to a large volume of sensitive, classified, and compartmented CIA documents. In order to provide the documents to the SSCI staff and ensure pertinent information was provided, the CIA established a review process. Initially, the SSCI staff provided search terms to the CIA RDI Review Team ("RDI team")[2] to identify responsive documents. The RDI team tasked Agency components with searching their databases for the requested material and collected the potentially responsive documents. The CIA tasked components of the Agency to conduct additional searches of their holdings for potentially responsive documents that were then provided to the RDI team. The RDI team reviewed the documents for responsiveness, removed information designated as Executive Privilege information, and provided the SSCI staff with access to the documents via the RDINet.

5. (U//FOUO) In an effort to understand the information the Agency had released and continued to release to the SSCI staff, the RDI Special Review Team (SRT) was created in May 2009. The SRT created documents known as Weekly Case Reports (WCRs), among other documents, at the request of then D/CIA Leon Panetta for the purpose of summarizing for CIA management the information being produced to the SSCI. In approximately February or March 2010, WCR production was halted by members of the Agency staff in response to a Department of Justice investigation led by Assistant U.S. Attorney John Durham.[3] Agency staff interviewed by CIA OIG interpreted the "Panetta Review" (a.k.a. Panetta Report) as a compilation of the WCRs.

(U) RDINet System

6. (U//FOUO) To facilitate SSCI staff access to the large number of released documents, the CIA created a computer network called RDINet. RDINet was established in a secure CIA vault in the [redacted] of the CIA's [redacted] building, with separate physical locations for CIA analysts to review and redact responsive documents and a physical "reading room" for SSCI staff to review responsive documents. The SSCI Majority and Minority staffs

[1] (U//FOUO) The Senate has historically referred to this as a study on the CIA's Detention and Interrogation Program. The study was launched following then D/CIA Michael Hayden's disclosure of the program to the SSCI in September 2006. On 5 March 2009, the SSCI voted to initiate a comprehensive review of the program.

[2] (U//FOUO) The RDI Review Team has had several historical names, including the Director's Review Group and the Office of Detainee Affairs. The team included attorneys from the Office of General Counsel that oversaw the RDI review performed by SSCI and an information technology team that supported the RDI system used for review.

[3] (U//FOUO) In January 2008, Assistant U.S. Attorney John Durham was appointed by the DOJ to lead an investigation into the destruction of videotapes of the interrogation of detainees. In mid-2009, the Durham task force was expanded to include a review of the detention and the use of various interrogation techniques by the Agency.

APPROVED FOR RELEASE DATE 14-Jan-2015

were later physically separated into two secure reading rooms at the request of the SSCI. Each of these offices included secure CIA-provided computer workstations for the review of materials released by the CIA and for the creation of individual work product.

7. (U//FOUO) RDINet is a standalone network that has a limited connection to the Agency Data Network (ADN) for administration purposes, including the ingestion of system software patches and updates and for routine network monitoring (Exhibit B). The SSCI and CIA were provided shared storage areas on RDINet that physically reside on the same hard drive array. Separate electronic storage drives were established for both the CIA and the SSCI to save documents and their respective reports. The SSCI was also provided additional storage drives further segregated between the Majority and Minority staff. Access to data was restricted through the use of access control lists and logical rules associated with the software. This virtual separation was intended to control access by the various parties to the RDINet, e.g., to prevent general CIA RDINet users from observing or accessing SSCI data, and to prevent SSCI users from observing or accessing CIA data that had not been released to them. Lotus Notes was installed on the network to provide an internal RDINet email capability. The email server allowed for communication among all RDINet users, both CIA and SSCI, and had no connectivity to the ADN.

8. (U//FOUO) From inception, the Office of General Counsel (OGC) was charged by the Agency with overseeing and supporting the RDI Program review.

9. (U//FOUO) In October 2013, when General Counsel Stephen Preston departed, was appointed the Acting General Counsel. Because had previously recused from any RDI matters,

Because of recusal regarding the RDI matter, was unsupervised by the Office of General Counsel pertaining to this matter.

10. (U//FOUO) On 22 June 2009, SSCI staff members began their review of RDI materials at the secure facility.

11. (U//FOUO) In November 2012, the RDI team learned of a vulnerability with the Google appliance, related to configuration settings that had been in place since the initial installation in November 2009. OIG reviewed an April 2013 email between members of the RDINet IT staff detailing the existing settings, which indicated an access control deficiency for search results. The RDI IT team updated the Google appliance in April 2013 to reflect this change. Prior to this update, the settings provided to OIG showed that the Google appliance was not configured to enforce access rights or search permissions within RDINet and its holdings.

C06274838

APPROVED FOR RELEASE DATE: 14-Jan-2015

12. (U//~~FOUO~~) On 1 November 2012, SSCI emailed of the RDI IT staff, and others to inform them that the new Google appliance was indexing the Majority staff work product on a shared drive. requested that the IT staff configure the tool to stop indexing the shared drive. OIG found that the Agency did not take action to address request.

(U) Memorandum of Understanding Regarding the Operation of RDINet

13. (U//~~FOUO~~) During the course of this investigation, OIG determined that a signed and finalized Memorandum of Understanding (MOU) between the SSCI and the CIA on the RDI review, including access controls, did not exist. Nevertheless, multiple interviewees referred to the existence of a signed MOU. In this regard, OIG found that that a series of written letters were exchanged between SSCI (Chairman Feinstein, then Vice Chairman Bond and then and CIA (then D/CIA Panetta and then) detailing the desires of each side with regard to the use of CIA space and systems, and SSCI access to documents (Exhibit C). These letters were found to contain some common language with regard to the use of the CIA facilities and computer systems.

14. (U//~~FOUO~~) The last letter OIG found on the topic from then D/CIA Panetta to Chairman Feinstein, dated 12 June 2009, described that "an agreement was reached between CIA and SSCI staff personnel regarding operating procedures for the SSCI review of material related to the CIA's detention and interrogation programs." The standard operating procedures (SOPs) referenced appeared to be detailed in a document titled "Standard Operating Procedures for SSCI Review,"[4] a three-page, 18-point document produced to OIG by the Office of General Counsel (Exhibit C.e). Point five of the document discussed the Committee's need to "create work product on a walled-off network share-drive" accessible only by the SSCI, and "CIA access to the walled off network shared drive will be limited to CIA information technology staff, except as authorized by the Committee or its staff." Point eight stated that all Committee staff granted access to the Reading Room were required to receive a security briefing. OIG reviewed a document titled "Security Briefing," dated "May 2009," but found no evidence that the briefing was ever provided to SSCI staff participating in the RDI review.

15. (U//~~FOUO~~) A separate document, titled "Memorandum of Understanding Senate Select Committee on Intelligence's Review of CIA's Detention and Interrogation Program,"[5] (Exhibit C.a), dated 28 May 2009, stated in point "C." that,

> A specially designed share-drive will be provided on the Agency's stand-alone network. As SSCI requires, the share-drive can be segregated with only SSCI access and walled-off CIA IT administrators, except as otherwise authorized by SSCI [sic].

[4] (U) Author unknown. The OIG did not find evidence that this document was provided to the SSCI.
[5] (U) Agency author. The OIG did not find evidence that this document was provided to the SSCI.

C06274838

APPROVED FOR RELEASE DATE: 14-Jan-2015

OIG found no evidence that this document was provided to the SSCI staff involved in the review or signed by either party. An email provided to OIG in relation to this document, from then to several CIA officers on 27 May 2009, stated that the document was a "proposed MOU that we will attempt to finalize with the SSCI staff." The email made reference to having SSCI staff sign a Nondisclosure Agreement (NDA) as well. OIG was not able to find any documentation that SSCI staffers signed an Agency NDA.

(U) Monitoring

16. (U//~~FOUO~~) The RDINet desktops were built as modified versions of the standard Agency workstations. At the time of inception, software security measures were put in place by the CIA to protect classified information from exploitation, including the and a logon warning banner. Both were standard features that were part of any Agency workstation.

17. ~~(S//NF)~~

(Exhibit D).

OIG found no evidence that SSCI members had been briefed on monitoring specific to RDINet.

18. (U//~~FOUO~~) The RDINet warning banner is the standard Agency warning banner. It consists of an advisement that all users are exposed to at the time of each login, which included any SSCI user who logged onto the RDINet. The warning is located in a dialogue box that the user has to acknowledge prior to logging in. The dialogue box consists of the following text:

> This is a U.S. Government system and shall be used for authorized purposes only. All information on this system is the property of the U.S. Government and may not be accessed without prior authorization. Your use of this system may be monitored and you have no expectation of privacy. Violation of system security regulations and guidance may result in discipline by the Agency, and violators may be criminally prosecuted.

(U) Acting General Counsel Department of Justice Crimes Report

19. (U//~~FOUO~~) On 7 February 2014, CIA Acting General Counsel wrote to Attorney General, Eric Holder, to report the matter of potential violation of Title 18 USC § 1030 (Fraud and Related Activity in Connection With Computers) by members of the

C06274838

APPROVED FOR RELEASE DATE 14-Jan-2015

SSCI on the RDINet[6] (Exhibit E). The report detailed that in the November 2010 timeframe, a member of the SSCI staff conducted a search on the RDINet that appeared intended to access a part of the system to which the member did not have authorized access.

IV. (U) INVESTIGATIVE FINDINGS

(U) Executive Summary of Investigative Findings

20. (U//FOUO) OIG investigation found support for allegations that CIA staff intentionally accessed the SSCI shared drive without authorization and exceeded authorized access. Additionally, three members of the RDINet IT team were not candid with OIG when interviewed and initially failed to disclose their recent investigative access to the SSCI shared drive. The investigation did not find support for the allegation that CIA performed real-time interception of SSCI communications for its review of the matter in question, however, CIA did review stored information that included and a review of some of the emails of SSCI Majority staff members on that network. The investigation found that D/CIA Brennan did not authorize the access or know the extent of the access, and OIG obtained conflicting testimony regarding whether or not D/CIA Brennan had any knowledge of a review performed on the SSCI shared drive until after it was completed. OIG investigation further found that the Director of Security authorized a review of the SSCI activities, including the reconstruction of the emails of SSCI staffers, following a stand-down order by the D/CIA and a request to withdraw authorization by the SSCI security officer. Finally, OIG investigation found that the CIA referral of criminal conduct by SSCI staffers was predicated on inaccurate information provided to the then-Acting General Counsel.

(U) Absence of a Formal Memorandum of Understanding Regarding the Operation of RDINet

21. (U//FOUO) OIG did not find evidence that a final document was agreed upon by both the SSCI and CIA, nor any documentation that an agreement was signed by the CIA or the SSCI. OIG did find, however, that there was a common understanding reached between the CIA and the SSCI. Several letters between SSCI Chairman Feinstein, then SSCI Vice Chairman Bond, and then D/CIA Panetta were exchanged in 2009 that contained enough similar language to define a working agreement. The common understanding between the SSCI and CIA did contain language regarding a walled-off network shared drive for exclusive SSCI use, except when IT staff required access for maintenance or troubleshooting. In addition to the working agreement, the SSCI staff were provided a warning at each login that their "use of this system may be monitored and you have no expectation of privacy." OIG found that the installed at the outset of RDINet by CIC was connected in the normal course of business and was collected in a manner consistent with the administration of

[6] (U) Pursuant to Section 1.6(b) of Executive Order 12333, as amended, and Sections VI.B, VII.A.4, and VIII.A of the 1995 Crimes Reporting Memorandum of Understanding between the Department of Justice and the Intelligence Community, the CIA is required to the report to the DOJ information concerning federal crimes.

C06274838

APPROVED FOR RELEASE DATE: 14-Jan-2015

Agency information systems. Additionally, OIG did not find documentation that NDAs or security briefings were provided to or signed by the SSCI staff.

(U) Unauthorized CIA Access to RDINet and Related Taskings

22. (U//~~FOUO~~) During the course of the investigation, OIG found that in January 2014, five Agency officers exceeded authorized access or directed such access to the SSCI side of RDINet. These accesses were not conducted as part of IT administration or routine Agency monitoring, but as part of a CIA investigation into how SSCI staffers obtained copies of documents referred to as WCRs.

23. (U//~~FOUO~~) the OGC attorney told OIG that became suspicious of an apparent security breach on the RDI system in December 2013. suspicions stemmed from letters from SSCI Chairman Feinstein and Senator Udall requesting copies of the "Panetta Review," the latter of which Senator Udall used to explain the reason for delaying Caroline Krass' confirmation hearing as CIA General Counsel. supposed that the "Panetta Review" referred to SRT documents or WCRs that were created at the behest of then D/CIA Panetta. As a result, told OIG began to consider the circumstances of how SSCI could have obtained access to CIA documents considered to be inappropriate. Between late December 2013 and early January 2014, expressed suspicions to and informed that the RDINet logs should be reviewed to determine how SSCI obtained access to the WCRs. OIG review of titled "Memorandum for the Record re: partial timeline of events surrounding discovery of SRT documents on RDI NET," ("MFR") (Exhibit F) which contained a timeline of events from perspective. In this document unilaterally reached the legal conclusion that had the legal authority to task members of to access the SSCI shared drive and look for Agency documents to which believed the SSCI staffers were not entitled. stated that tasked the IT team to look for SRT documents on the SSCI staff side on 9 January 2014.[7]

(U) RDI IT Team Review

24. (~~C//NF~~) On 9 January 2014, after a discussion with directed RDINet IT, to set up a user profile on RDINet that was configured with the same privileges as a SSCI Majority staff user. requested this access in order to run Google queries with the same permissions as a SSCI staffer to see what they were able to view in their search results. identified the presence of WCR reports on the SSCI Majority shared drive through a review of the Google search results. After identifying the documents, mapped to the folder where the documents resided and used "dummy account" with SSCI-like permissions to

[7] (U//~~FOUO~~) was initially interviewed by OIG prior to the discovery of the MFR. Following the discovery of the MFR, declined to be interviewed about its contents.

APPROVED FOR RELEASE DATE: 14-Jan-2015

open the folder. recognized the documents as likely WCR reports based on their filenames and folder structure, and opened "a few" of the documents to view the first page, where observed a disclaimer and format similar to the WCR documents. informed of the findings. briefed and on the findings.

25. (U//~~FOUO~~) On 10 January 2014, tasked to search the RDINet database to verify whether the SSCI had been provided access to the restricted documents. search of the database revealed that the documents were not located in the database and they concluded that they had therefore not been produced by the CIA to the SSCI for review. Following search, conducted a search on the root of the RDINet shared drive, which contains all user profiles, user accounts, and shares used by both CIA and SSCI users. search indicated that the restricted documents were located on the SSCI Majority shared drive and one SSCI user's personal drive. navigated directly to the locations of interest on the SSCI Majority shared drive as well as to the SSCI user's personal drive.

26. (U//~~FOUO~~) During the course of the investigation, OIG received conflicting statements from regarding additional accesses to the SSCI shared drive and subsequent screenshots taken during those accesses. According to following confirmation that the restricted documents were present on the SSCI Majority shared drive, specifically requested access to the drive so that could look at the documents granted this access, associating the drive as workstation, for approximately 20 minutes. stated that, during this time, captured screenshots of the SSCI Majority shared drive file structure. emailed the screenshots to requesting the screenshots be transferred to the ADN. According to however, requested that come to office, where provided access to the SSCI Majority shared drive from workstation. when interviewed, was unsure of the methods used to grant the access and stated that helped take screenshots of folders and sub-folders of interest on the SSCI Majority shared drive on behalf.

27. (U//~~FOUO~~) OIG review of activity associated with RDINet user account on 10 January 2014 showed attempts were made to access Next, activity showed usage of followed by a Lotus Note to ADN. A review of personal storage drive on the ADN found a folder named which contained related to searches of the SSCI Majority shared drive, home page, and "not authorized" messages.

28. (U//~~FOUO~~) provided the screenshots to and tasked to determine if the restricted documents had been accessed by SSCI staffers. On 10 January 2014,

C06274838

APPROVED FOR RELEASE DATE: 14-Jan-2015

tasked by email to obtain The email acknowledged that this was a SSCI shared drive.

29. (U//~~FOUO~~) On 12 January 2014, sent an email to the RDINet IT team requesting new versions of the screenshots that showed Q:\ as the mapped drive letter vice Y:\. SSCI user access to the drive was mapped as requested these updated screenshots in order to "provide the optic" (e.g. display more accurately) that the folder was located on the SSCI Majority shared drive. Both complied with the request and emailed responses on 13 January 2014.

30. (~~C//NF~~) At OIG's request, provided OIG an email and attachments dated 13 January 2014 from to and copying The email documented the RDINet IT team's response to 12 January tasking and contained snapshots of the contents of the folder properties and security settings for a document titled "WCR MJA," and a capture of the virtual folder "My Computer", showing the drive Q:\ labeled as "Share Majority Data." also responded to a series of questions from regarding the number of files in and in its subfolders, as well as information regarding SSCI privileges on RDINet.

31. (U//~~FOUO~~) Between 5 June and 13 June 2014, OIG and Senate Sergeant-at-Arms conducted a joint forensic review of the RDINet log data. The review determined that relevant logs containing file access and security information were not retained appropriately[8]. A review of file meta-data did not show any CIA users as having altered the WCR documents contained in the Q:\ drive, but did not contain sufficient information to assess access by CIA users.

32. (~~C//NF~~) During the course of the investigation, OIG determined that RDINet IT officers were not forthcoming in their initial interviews with OIG, having failed to disclose the assistance they provided to in the searches of RDINet between 9 and 13 January 2014. As a result, OIG requested second interviews with each officer. complied with the second interview requests and admitted to the conduct when confronted with the information from the emails; declined a second interview.

(U//~~FOUO~~) *Review*

33. (~~S//NF~~) OIG investigation found that on 10 January 2014, tasked to conduct a review of activity on the SSCI side of RDINet. As a part of the review requested by ran queries against previously archived RDINet data to determine whether the documents in question had been accessed by SSCI staff. The date

C06274838

APPROVED FOR RELEASE DATE: 14-Jan-2015

range of the review focused on the 2010 to 2013 time period. as a part of any of the activities in question during the January 2014 time frame. all data reviewed by at the request of the RDI team was historically logged information.

34. ~~(C//NF)~~ In multiple communications with stated that the requests for review were being made on behalf of D/CIA Brennan. On 9 January 2014, called CIC alerting to a forthcoming "D/CIA tasking". tasked by email on the morning of 10 January 2014, requesting that the team provide contained in the folder of RDINet for the period 1 March 2009 to 31 December 2013. replied to the email, stating that the D/CIA wanted the results of the review that afternoon. provided a response in the form of an Excel spreadsheet on the afternoon of 10 January 2014. Following receipt of this information, emailed and stated that the D/CIA had requested for the same folder and requested a response by Monday, 13 January 2014. On 13 January, provided with an Excel spreadsheet of the requested On the afternoon of 13 January 2014, tasked with determining the provenance of the documents contained in the aforementioned folder. This task was not completed, as D/CIA Brennan directed that no further work be performed by at a meeting on 14 January 2014.

35. ~~(U//FOUO)~~ Despite representations by CIC that D/CIA Brennan directed the aforementioned taskings to OIG did not find evidence to support any such direction.

36. ~~(U//FOUO)~~ Due to conflicting information obtained by OIG through the course of the investigation, OIG could not determine whether any of D/CIA Brennan's senior staff, much less the D/CIA himself, approved any of the taskings made to In mentioned consulting with and and informing them that would be tasking to determine if the documents were accessed by SSCI users. Neither nor recalled approving any tasking, and OIG did not identify documentary evidence confirming any approvals.

37. ~~(U//FOUO)~~ D/CIA Brennan told OIG that he first learned of the concerns regarding documents on RDINet from on the evening 9 January 2014. D/CIA Brennan stated that he recalled referring to a review of but that he did not recall if explained how anyone knew the location of the documents. Subsequently, D/CIA Brennan spoke to on 10 and 11 January 2014. According to D/CIA Brennan tasked to "use whatever means necessary" to find out how the documents had ended up on the SSCI shared drive. D/CIA Brennan told OIG that he only asked "are we sure" that the documents were CIA documents and that he wanted to better understand the RDINet system architecture.

C06274838

APPROVED FOR RELEASE DATE: 14-Jan-2015

38. (U//~~FOUO~~) OIG presented D/CIA Brennan with an excerpt from the "MFR" document found on [redacted] D/CIA Brennan told OIG that there appeared to be a difference in emphasis between what he had told [redacted] and what [redacted] documented. In response to whether he told [redacted] to proceed by "whatever means necessary," D/CIA Brennan stated that he would never use those words and had not stated that to [redacted] D/CIA Brennan further stated that he was only interested in gaining knowledge of the system because he was unsure if it was a closed system. D/CIA Brennan stated that he had "tremendous respect" for [redacted] and added that he counted on [redacted] action to be consistent with legal authority. D/CIA Brennan reiterated that he had understood that CIA documents were found via [redacted] D/CIA Brennan stated that he wanted to know how the documents got to the SSCI side but did not direct anyone to review SSCI systems.

39. (U//~~FOUO~~) A meeting was held in the Director's conference room in the afternoon of 14 January 2014, attended by D/CIA Brennan, [redacted] CIC), Neal Higgins (Chief/Office of Congressional Affairs), [redacted] Executive Director Meroe Park, and others. At this meeting, D/CIA Brennan expressed surprise and concern at the presence of CIC officers. Several witnesses told OIG that D/CIA Brennan was upset that CIC had been engaged in the inquiry, and was concerned about the optic of the counterintelligence arm of the Agency investigating the activity of SSCI staffers. D/CIA Brennan stated he was surprised at the work that had already been performed, and explicitly told everyone at the meeting not to do anything else on the "tech or forensic side." D/CIA Brennan told OIG that he did not task the [redacted] review, and that there should not have been any other work performed after the meeting on the 14 January 2014. D/CIA Brennan confirmed with OIG that he was surprised when he learned CIC [redacted] was involved in the review.

(U) Office of Security Cyber Blue Team Review

40. (U//~~FOUO~~) During the meeting on 14 January, D/CIA Brennan gave the order to "stand down" on any further reviews until he could brief the SSCI on the Agency's concerns and the actions taken to date. On 15 January, D/CIA Brennan briefed the SSCI and proposed a joint review between the Agency and SSCI Security [redacted] D/CIA Brennan stated that he did not think that Chairman Feinstein explicitly agreed to a joint review that day, but did not explicitly say no or dismiss the conversation. D/CIA Brennan thought that Chairman Feinstein wanted to talk to [redacted] about it and consider the idea further. D/CIA Brennan stated that he did not task anything after this meeting with the SSCI, and that it should have been abundantly clear after the meeting on 14 January in his conference room that all work should have stopped.

41. (U//~~FOUO~~) Between 16 and 17 January 2014, the CIA-Office of Security Cyber Blue Team[9] conducted a review of the RDINet [redacted] in [redacted] holdings and produced

[9] (U//~~FOUO~~) The Cyber Blue Team, established in February 2013, identifies vulnerabilities and risks, quantifies impacts to make educated decisions, and partners with other organizations in order to mitigate risks, among other duties.

C06274838

APPROVED FOR RELEASE DATE: 14-Jan-2015

a report dated 17 January 2014. Office of Security, told OIG that first became aware of the SSCI events on 15 January 2014, when contacted at home to inquire what it would take to conduct a security review. OIG confirmed that was not present at the 14 January 2014 meeting with D/CIA Brennan, and was not aware of the standdown order. stated that spoke to who explained to that SSCI staff accessed data they were not authorized to access. stated that spoke to on 15 January 2014, and that was planning to work with on a joint security review of the RDINet. On 16 January 2014, emailed to request concurrence on the plan of action developed by the Office of Security. Also on 16 January, received an email from stating that they were on "stand down" for a joint security review. On 17 January 2014, responded to request for concurrence "...there has been a new development" and requested, "If you can come to the Director's Office around 8am that would be ideal." OIG did not find any response to request for concurrence.

42. (U//~~FOUO~~) sent an email to Higgins and copied on 16 January 2014 and stated that SSCI Chairman Feinstein would be sending a letter to the D/CIA the following day requesting that no forensic examination of the SSCI "network" proceed. On 17 January 2014, Chairman Feinstein wrote to D/CIA Brennan and requested suspension of access to the computers and networks used by the SSCI and any forensic investigation planned by the CIA. Chairman Feinstein explicitly stated in the letter that until she could consider the matter further, D/CIA Brennan did not have her agreement for any investigative activity.

43. (U//~~FOUO~~) told OIG that on 16 January instructed the Cyber Blue Team to review the RDINet stated that did not seek approval because it was CIA information on a CIA network. further stated that this was a normal function for the Cyber Blue Team, capable of performing such a review. stated that did not feel that was out of coordination with CIA leadership at any time. On 16 January 2014 emailed and advised that the SSCI Chairman was drafting a letter to the Director of the CIA requesting to stop the entire plan of action for the joint review. described the "full plan of action" to OIG as the imaging of RDINet and a full forensic review and stated that interpreted this as a request to stop the joint forensic investigation. did not believe that the request applied to the review of or that the Cyber Blue Team review was akin to forensic activity.

44. ~~(S//NF)~~ On 17 January, the Cyber Blue Team met with to review the forensic generated by the SSCI staff, including reconstructed emails between SSCI staff on the SSCI side of RDINet. The Cyber Blue Team Report, detailed the team's evaluation of RDINet system data surrounding the documents in question. The report stated that a "Congressional user" was able to navigate directly to a "shared directory" and access documents never intended for dissemination to "Congressional users." The report stated that the user first accessed the directory on 9 November 2010, and copied the data contained

C06274838

APPROVED FOR RELEASE DATE: 14-Jan-2015

within to another shared directory. The report detailed further activity performed by a "Congressional user" on 24 June 2011 including copy/paste, keyword searches, and communication between "Congressional users" that directed them to review specific documents. As mentioned previously, OIG did not investigate the activity of the SSCI staff.

(U) Department of Justice Crimes Report

45. (U//~~FOUO~~) On 7 February 2014, then-Acting General Counsel [redacted] sent the Department of Justice a Crimes Report (Exhibit E) that detailed a "limited security investigation." [redacted] wrote that a search tool installed on the system in question had a vulnerability that was exploited by SSCI staff members to view and retrieve documents on a part of the system to which they did not have access. Further, [redacted] explained that the file path to a document discovered while using the search tool could be copied and pasted into a browser access bar as a URL, which would give the user access to that document. The explanation stated that the user could bring a copy of the document across the system's firewall and paste it into a folder on the other side of that firewall. [redacted] wrote that the information made available to [redacted] indicated that a "non-employee" copied a URL, pasted it into the browser's access bar, and accessed the document, repeating this process numerous times. [redacted] told OIG that information provided by [redacted] was the sole source of information for the 7 February 2014 report.

46. (U//~~FOUO~~) OIG did not identify a factual basis to support [redacted] Department of Justice Crimes Report. OIG found that [redacted] had been provided inaccurate information on which the report was based.

47. (U//~~FOUO~~) [redacted] told OIG that the information [redacted] provided to [redacted] was predicated on the Cyber Blue Team Report that stated that a Congressional user was able to navigate directly to a shared directory not intended for access to Congressional users. However, the Cyber Blue Team report did not identify the vulnerability stated in [redacted] letter as the source of the documents. The source of the information cited by [redacted] was information provided to [redacted] orally by [redacted] was unable to verify the accuracy of the information provided by [redacted] or to review [redacted] legal conclusions regarding the authority to view the SSCI shared drive because he was recused from matters relating to RDI, including the Cyber Blue Team Report. In fact, [redacted] told OIG that he did not read the Cyber Blue Team report as [redacted] was informed that the report contained details of SSCI communication, which made [redacted] wary.

V. (U) DOJ COORDINATION

48. (U//~~FOUO~~) On 3 February 2014, Title 50 U.S.C. § 3517, OIG reported the matter of potential CIA officer violations of Titles 18 USC § 1030 (Fraud and Related Activity in Connection with Computers) and 2511 (Authorization for Interception of Wire, Oral, or Electronic Communications) to the Department of Justice. On 8 July 2014, DOJ wrote to inform the OIG that DOJ had completed its review of the allegations and had no prosecutorial interest.

C06274838

APPROVED FOR RELEASE DATE: 14-Jan-2015

(U) Other Related RDINet Events

1. (U//~~FOUO~~) The OIG learned of several historical incidents related to RDINet during the course of this investigation. The incidents were cited by multiple interviewees as demonstrating that SSCI users were previously aware of Agency monitoring of SSCI activity on RDINet.

2. (U//~~FOUO~~) In January 2010, the CIA RDI team removed 874 documents from the virtual Reading Room and an additional set of 52 documents on 11 May 2010. The CIA staff interviewed by the OIG stated that these documents were "Executive Privilege" documents that had been unintentionally comingled on the RDINet with documents intended for production to the SSCI. When it was discovered that these documents had been added to the virtual Reading Room in error, the RDI team removed the documents. On or about 11 May 2010, the RDI team informed SSCI that documents were removed from the virtual Reading Room. SSCI staffer sent an email to on 12 May 2010, stating that "Our understanding of the agreement we reached with you last year was that the computer systems on which the Committee would be working would only be accessed by CIA personnel for purely administrative, IT actions. CIA's actions in removing documents from our system are unequivocally not administrative." The RDI leadership then informed the relevant CIA employees that no further documents should be removed from the Reading Room prior to consulting with the SSCI staff.

3. (U//~~FOUO~~) In December 2009, the detected that a the SSCI staff In January 2010, the same individual also reported having a camera in the secure facility to the facility's gate guard but did not provide the camera for review. The individual was identified as on RDINet in November and December 2010. The matter was referred to the CIA Counterintelligence Center's Counterespionage Group (CEG), and the employee was removed from the team.

4. (U//~~FOUO~~) On 6 May 2010, a SSCI staffer requested from the Agency the ability to print a sensitive document from the RDINet. The SSCI staff member attempted to bypass the print restriction by CIC reviewed the incident and recommended removing the possibility of SSCI staffers utilizing but because the capability was it could not be removed or disabled. The RDI team discussed this issue with the SSCI staff and reminded them of the need for security of the sensitive documents.

5. (U//~~FOUO~~) In 2013, a number of detainee videos not provided to the SSCI by the CIA were requested by SSCI staff. The RDI review team evaluated the request and determined the videos to be outside of the scope of the SSCI review. According to the SSCI staffer asserted his request, saying he had a document that defined the location of the videos and that they were from responsive detainee sites. The staffer presented a hardcopy spreadsheet that recognized as a working copy produced by the SRT team. confirmed with the SRT analysts that the requested videos were not responsive, and that all of the responsive videos from the spreadsheet had already been provided. The

Approved for Release: 2024/02/27 C06274838

RDI IT team reviewed ways the SSCI staff could have accessed the spreadsheet and hypothesized that there may have been a Google search appliance vulnerability. The team discovered that the Google search appliance was capable of searching both the SSCI side as well as the RDI team's side of the Spartan Gate database. The results of Google searches showed documents from both the SSCI and Agency sides of RDINet and included a link to cached versions of the documents. When clicked, the cache link presented the text of the document in question. The RDI IT Team implemented a fix for this vulnerability in April 2013. The CIA requested that the document be destroyed in both paper and electronic format and the SSCI staffer agreed to do so.

Approved for Release: 2024/02/27 C06274838